PASSWORDS 101:
BUILDING STRONG FOUNDATIONS FOR DIGITAL SECURITY (PART 1)

Contributed by the Fairview Technology Advisory Committee

In today's digital age, passwords are our first line of defense against cyber threats. Yet, many people still use weak, easily guessable passwords, putting their personal information at risk. Imagine your online accounts as vaults holding your most valuable digital treasures. Weak passwords are like flimsy locks – easily breached by thieves. This article, the first of a two-part series, will guide you through the essentials of creating strong passwords and understanding their importance.

Strong Passwords Matter [1]

Just like you wouldn't leave your house unlocked, don't leave your online accounts vulnerable. Strong passwords are key to keeping your digital castle secure. By using strong, unique passwords, you significantly reduce the risk of unauthorized access to your accounts.

Long, Complex and Unpredictable [2]

A strong password is one that's easy for you to remember but difficult for others to guess. The ideal password strikes a balance between memorability and security. You may be tempted to use information that is easy to remember, such as names, birthdays or other personal information, but this should be avoided. Instead, passwords should use a combination of letters, numbers, cases, and symbols to form an unpredictable string of characters.

Tips for Creating a Strong Password[3]

1. **Use at least 12-16 Characters.** Longer passwords significantly reduce the likelihood of successful attacks. Aim for at least 12-16 characters for optimal security.

2. **Create or Use a Passphrase.** A passphrase is a sentence-like string of words used for authentication that is longer than a traditional password, making it easy to remember and difficult to crack. Examples of famous movie quotes turned into passwords include:

- Th3Y3llowBr1ckR0@d! (The Wizard of Oz)
- MayTh3F0rc3BWithU! (Star Wars)
- T0Inf1nity&BeYoNd! (Toy Story)

3. **Avoid Personal Information.** Do not use your name, birthdate, children's or pets' names or any personal information as your password.

4. **Avoid Using the Same Password for All Your Accounts.** Reusing passwords increases vulnerability. If a site gets hacked, your details and passwords can be leaked or sold. It is recommended to use different passwords for each account.

Managing Multiple Passwords[4]

With numerous accounts, it's tempting to reuse passwords, which increases vulnerability. Consider a password manager, which is a digital vault that generates and stores strong, unique passwords and unlocks them with ease for you to use. Accessing them is simple – using a single master password, or, for added convenience, unlock the password manager with biometric authentication like your fingerprint or face scan.

Utilize breach monitoring services to keep track of compromised passwords or email addresses and receive alerts if your information appears in a data breach.

Conclusion

Creating and maintaining strong passwords is essential for safeguarding your digital presence. Read Passwords 101 (Part 2) for more information about password management tools and multi-factor/two-factor authentication (MFA/2FA), which enhances security by requiring a secondary verification method. The article also discuss additional best practices to ensure your digital security.

Sources:

1 National Cybersecurity Alliance

2 Boston University

3 Cybersecurity and Infrastructure Security Agency

4 Carnegie Mellon University